Sécurisation des communications

Exercice 1 : Nombre de clés.

Un groupe de n personnes souhaitent communiquer entre elles, chacune, deux à deux. Elles souhaitent utiliser un moyen de communication sécurisé par un chiffrement symétrique. Combien de clés différentes seront nécessaires?

La première personne devra créer n – 1 clés, la seconde personne n – 2, … , la dernière 0 clé.

On a donc (n – 1) + (n – 2) + … + 0 = $\sum_{k=1}^{n-1} k = \frac{(n)(n-1)}{2}$

Exercice 2 : Méthode de chiffrement de Vigenère.

Si on appliquait cette méthode à un alphabet de 95 caractères (les caractères ascii) :

1. Combien de clés différentes peuvent exister avec 4 caractères?

   Il y a 95^4 clés possibles.

2. Combien de temps cela prendrait-il au maximum pour déchiffrer un message par recherche exhaustive (force brute), si le temps de calcul pour le déchiffrement est de 1 milliseconde par clé?

   On applique un ordre de grandeur au nombre de clés : $95^4 \approx 100^4 = 10^8$ clés possibles. On teste une clé en 1 ms = 0,001 s = 10^{-3} s. Donc $10^8 \times 10^{-3} = 10^5$ s ≈ 28 heures pour tous tester.

Exercice 3 : Mots de passe

1. Combien de mots de passe différents de 10 caractères peuvent être générés à l'aide des 95 caractères ascii?

   Il y a 95^{10} clés possibles.

2. Avec un ordinateur capable de tester 1 million de mots de passe par seconde, combien de temps cela lui prendra t-il pour explorer l'ensemble des combinaisons?

   On applique un ordre de grandeur au nombre de clés : $95^{10} \approx 100^{10} = 10^{20}$ clés possibles. On teste 10^6 clés par seconde donc il nous faut $10^{20} / 10^6 = 10^{14}$ secondes ≈ 3 millions d'années.

3. Expliquer ce qu'est une attaque par recherche exhaustive.

   Méthode algorithmique qui consiste principalement à essayer toutes les solutions possibles

4. Pour les propriétaires d'un site internet, vaut-il mieux conserver dans la base de données, les mots de passe des clients, ou bien le hachage de chacun de ces mots de passe?

   Les mots de passe ne doivent jamais être conservés en claire où que ce soit. Il faut donc conserver les hash.

Exercice 4 : RSA

1. (Optionnel) Quel est la valeur de 8^7 modulo 55? Appeler ce nombre n.

   $8^2 \equiv 64 \equiv 9 [55]$ et $(8^2)^3 \times 8 \equiv 9^3 \times 8 \equiv 5832 \equiv 2 [55]$

2. (Optionnel) Quel est l'inverse de n modulo 55? (rappel : $n \times inverse \equiv 1 [n]$)

   $2 \times 28 \equiv 56 \equiv 1 [n]$ Donc 28 est un inverse.

3. Dans un protocole de chiffrement asymétrique, les algorithmes de chiffrement et de déchiffrement sont-ils les mêmes?

   Les algorithmes sont les mêmes, les clés de chiffrement et déchiffrements sont différentes.

4. Dans un protocole de chiffrement asymétrique, toutes les personnes possédant la clé publique de Bob peuvent lui envoyer un message?

   Oui, ici la clé publique sert au chiffrement et seul Bob avec sa clé secrète pourra les déchiffrer.

5. Dans un protocole d'authentification, toutes les personnes possédant la clé publique de Bob peuvent vérifier sa signature émise ?

   Oui, ici c'est la clé de chiffrement qui est privée et possédée par Bob. La clé de déchiffrement est publique et tout le monde peut vérifier que c'est bien Bob qui signe les messages.

6. Supposons que Bob envoie à Alice un message chiffré de la manière suivante: C = chiffrement(m, Bob_public_key). Est-ce qu'Alice peut authentifier Bob avec ce message?

   Non, Bob doit utiliser sa clé privé pour chiffrer le message chiffrement(m, Bob_private_key). Alice utilisera dechiffrement(m,Bob_public_key) pour vérifier la provenance du message.

Exercice 5 : Man in the middle

1. Décrire les échanges qui ont lieux lors d'un échange de clé Diffie-Hellman intercepté par une attaque man in the middle.

   L'échange de clé Diffie-Hellman est vulnerable au man in the middle. Il suffit que toutes les communications d'Alice et Bob passent par Mallory, qui se fera passer pour Alice s'il communique avec Bob et pour Bob s'il communique avec Alice.

   Alice ↔ Mallory ↔ Bob

   Mallory procédera à deux échanges de clés et décryptera les messages d'Alice pour les envoyer à Bob et vice versa.

2. Décrire une tentative d'attaque man in the middle sur un protocole HTTPS.

   Il est impossible de réaliser une attaque man in the middle sur le protocole HTTPS. Si Alice tente d'accéder au site web de Bob mais que Mallory intercepte la requête, Mallory doit renvoyer un certificat d'authentification qui contient normalement la clé publique de chiffrement pour communiquer avec le serveur de Bob. Or ce certificat est signé par une autorité de certification et toute modification du certificat sera repéré par Alice.